Diese Website verwendet Cookies von Google, um Dienste anzubieten und den Traffic zu analysieren. Deine IP-Adresse und dein User-Agent werden zusammen mit Messwerten zur Leistung und Sicherheit für Google freigegeben. So können Nutzungsstatistiken generiert, Missbrauchsfälle erkannt und behoben und die Qualität des Dienstes gewährleistet werden.

WEITERE INFORMATIONEN OK

Tuesday, October 25, 2005

Anti-phishing bills and "unauthorized access"

The spate of anti-phishing bills currently making their way into or through legislative bodies around the world provide a good opportunity to do something that is long overdue -- amend our obsolete and destructive cybercrime statutes. If network security professionals are to be empowered to stop phishing and prevent cyberterrorism, a major overhaul to these statutes is crucial.

The Cuthbert case in the U.K. has provided yet another example of an unjust conviction under cybercrime statutes. These statutes were typically enacted before the advent of the Web and generally make "unauthorized access" to a computer a crime. Under these statutes, the Web equivalent of pushing on the door of a grocery store to see if it's still open has been made a crime. These vague and overly broad statutes put security professionals and other curious web users at risk. We depend on network security professionals to protect us from cyberterrorism, phishing, and many other on-line threats. These statutes, as currently worded and applied, threaten them with career ruin for carrying out their jobs. Cuthbert was convicted for attempting to determine whether a web site that looked like British Telecom's payment site was actually a phishing site, by adding just the characters "../.." to the BT site's URL. If we are to defeat phishing and prevent cyberterrorism, we need more curious and public-spirited people like Cuthbert.

Meanwhile, these statutes generally require "knowledge" that the access was "unauthorized." It is thus crucial for your future liberty and career that, if you suspect that you are suspected of any sort of "unauthorized access," take advantage of your Miranda (hopefully you have some similar right if you are overseas) right to remain silent. This is a very sad thing to have to recommend to network security professionals, because the world loses a great deal of security when security professionals can no longer speak frankly to law-enforcement authorities. But until the law is fixed you are a complete idiot if you flap your lips. Since almost any online activity of which, it turns out, the web site operator does not approve may be deemed to be "unauthorized," these cases revolve around whether the defendant "knew" that the act was "unauthorized." In Cuthbert's case, because he told the police that his purpose had been to test the public site's access controls (the equivalent of pushing on doors of a grocery store to see if it is open) to see if he had just given his credit card number to a phishing site -- a laudable act of due diligence in this age of phishing and identity theft -- he essentially admitted to the difficult knowledge element of the criminal statute. After that, the conviction was a slam dunk.

Several years ago, network security professional Randall Schwartz engaged in a traditional friendly competition with security professionals in another company to try to find holes in their security. That company turned out to be not so friendly and Schwartz was convicted under an Oregon statute similar to the one that felled Cuthbert. The court rejected a defense of unconstitutional vaguenessbecause, said the court, it sounded more like a defense of overbreadth. In fact these statutes are both vague and overbroad, but courts often do not understand the issues involved.

Pages

- Home

About Me

Nick Szabo

"A premier thinker about history, law and economics, and the lessons they have for security." -- Adam Shostack, Emergent Chaos

"Szabo comes out with these essays that leave me in awe." -- Brian Dunbar

"Reading material that is eclectic, challenging and endlessly fascinating." -- Sean McGrath, Propylon

"Like most blogs worth my attention, this blog is updated only infrequently. That is because the authors of blogs worth my attention only post when they have something to say that is true, relevant and not already known by their audience. Most of the human race does not have the skill to know when an idea has these three properties. The skill is particularly rare in the fields of politics and economics, which is why this blog is such a rare and valuable thing." -- Richard Hollerith

View my complete profile

Orin Kerr (a professor at my law school) has written a good paper on the subject with respect to laws in the United States.

Kerr recommends using more specific language instead of "unauthorized access." My own recommendation is that, if we are going to keep the "unauthorized access" language, it at least should be amended along the following lines:

(1) an access should not be defined as "unauthorized" unless either the defendant was provided notice of lack of authorization (equivalent to a no-trespassing sign) and affordance (a barrier that requires some intentional act to pass, equivalent to a fence or a door), or there is a long-standing and widely-known custom that the kind of access as perceived by the defendant was unauthorized, or both, and
(2) there should be no crime unless there was an underlying intent to use the unauthorized access to commit another kind of crime (such as theft of data, trespassing via disruption of computer operation, etc.)

Under (1), "unauthorized access" would for the first time have a clear definition, similar to how "trespassing" is defined in the context of a public place (you are authorized to enter a public store when it is opened, to push on the door to see if the store is open, to shop, in some jurisdictions to use the restroom unless there is a sign to the contrary; but you are not to enter the back room where they have the safe). Security professionals would operate under the same rules as everybody else instead of having knowledge discriminatorily imputed to them because they are "supposed to know better."

Under (2), accesses done for laudable purposes, such as Cuthbert's investigation about whether his credit card had been phished, would no longer be considered criminal. Network security professionals would be freed to do their jobs and protect the Internet from real criminals.

The current spate of anti-phishing bills currently making their way into or through legislative bodies around the world provide a good opportunity to amend cybercrime statutes -- to bring them into the twenty-first century world of the public web.

Posted by Nick Szabo at 11:31 AM

2 comments:

lang said...

Hmm, no trackback? Here's a manual trackback to my post.

BTW, I wouldn't expect too many comments here - the blog comment security system is too hard to navigate.

7:47 AM

Nick Szabo said...

Thanks for the feedback. I've enabled the "links to this post" feature.

12:37 PM

Post a Comment

Blog Archive

- ► 2018 (1)
- ► 2017 (3)
- ► 2016 (4)
- ► 2015 (3)
- ► 2014 (3)
- ► 2013 (3)
- ► 2012 (8)
- ► 2011 (12)
- ► 2010 (9)
- ► 2009 (29)
- ► 2008 (55)
- ► 2007 (47)
- ► 2006 (130)
- ▼ 2005 (44)
  - ► December (16)
  - ► November (5)
  - ▼ October (23)
    - Software patents paper
    - Supreme Court takes patentable subject matter case...
    - Automobile privacy
    - Are intellectual property rights natural?
    - Civil liberties in the forever war
    - Negative rights and the United States Constitution...
    - Patent law reform in the U.S.
    - Janice Rogers Brown
    - Blackberry e-mail injunction
    - Anti-phishing bills and "unauthorized access"
    - Patents and borders
    - A world of vouchers
    - New writing -- The Birth of Insurance
    - Manual of Patent Examining Procedure (MPEP)

Subscribe to: Post Comments (Atom)

Surveillance and technological "neutrality"

Cuthbert: "unauthorized access"

Information, randomness, and cryptography

Rights of travel

Some common and natural law rights of parenthood

Common law rights

Unenumerated

A Measure of Sacrifice

Shelling Out -- The Origins of Money

Simple theme. Powered by Blogger.